**Załącznik nr 6 do SWZ**

**Rozdział I: Założenia początkowe oraz wymagania ogólne**

1. **Wprowadzenie** 
   1. Przedmiot zamówienia jest realizowany w ramach grantu pn. „Cyberbezpieczny Samorząd” współfinansowanego ze środków Unii Europejskiej: Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2. - Wzmocnienie krajowego systemu cyberbezpieczeństwa, Fundusze Europejskie na Rozwój Cyfrowy 2021-2027.
   2. Realizacja grantu ma na celu zwiększenie bezpieczeństwa informacji poprzez wzmacnianie odporności jednostek samorządu terytorialnego (JST) oraz ich zdolności do skutecznego zapobiegania incydentom bezpieczeństwa teleinformatycznego, wykrywania ich i reagowania na nie.
2. **Ogólny opis przedmiotu zamówienia** 
   1. Przedmiot zamówienia obejmuje sprzęt, oprogramowanie oraz szkolenia podnoszące poziom cyberbezpieczeństwa:

|  |  |  |
| --- | --- | --- |
| Lp. | opis | realizacja w ramach etapu: |
| 1 | Dostawa, wdrożenie, instalacja serwera I, instruktaż z zakresu administracji i bieżącej obsługi | II |
| 2 | Dostawa, wdrożenie, instalacja serwera II, instruktaż z zakresu administracji i bieżącej obsługi | I |
| 3 | Dostawa, wdrożenie systemu do ochrony brzegu sieci klasy UTM, instruktaż z zakresu administracji i bieżącej obsługi dostarczonego systemu UTM | II |
| 4 | Dostawa, wdrożenie, instalacja Biblioteki taśmowej, instruktaż z zakresu administracji i bieżącej obsługi dostarczonego systemu | I |
| 5 | Dostawa, wdrożenie sieciowego serwera plikowego typu NAS, instruktaż z zakresu administracji i bieżącej obsługi dostarczonego sprzętu – 2 szt. | I |
| 6 | Dostawa, wdrożenie Oprogramowania do przeciwdziałania wyciekom danych dla 100 użytkowników, instruktaż z zakresu administracji i bieżącej obsługi dostarczonego systemu | II |
| 7 | Dostawa, wdrożenie, instalacja przełącznika sieciowego, instruktaż z zakresu administracji i bieżącej obsługi dostarczonego systemu – 2 szt. | I |
| 8 | Dostawa, wdrożenie, instalacja oprogramowania do wykonywania kopii zapasowych, instruktaż z zakresu administracji i bieżącej obsługi dostarczonego systemu | III |
| 9 | Dostawa, wdrożenie, instalacja oprogramowania umożliwiającego monitoring usług i systemów użytkowanych przez Zamawiającego wraz z możliwością wysyłania powiadomień e-mail/sms, instruktaż z zakresu administracji i bieżącej obsługi dostarczonego systemu | I |
| 10 | Dostawa, wdrożenie, instalacja oprogramowania umożliwiającego bezpieczne przetwarzanie danych w środowisku hybrydowym: praca w Urzędzie, praca zdalna, współpraca z jednostkami podległymi, instruktaż z zakresu administracji i bieżącej obsługi dostarczonego systemu | III |
| 11 | Szkolenia specjalistyczne z zakresu cyberbezpieczeństwa dla administratorów IT wyznaczonych przez Zamawiającego – 2 osoby | III |
| 12 | Szkolenia z zakresu cyberbezpieczeństwa dla pracowników Zamawiającego – 80 osób | II |

* 1. Przedmiot zamówienia musi być dostarczony, wdrożony i zainstalowany w całości w siedzibie Zamawiającego we wskazanym miejscu.
  2. Usługi projektowania, instalacji, konfiguracji i wdrożenia Wykonawca musi przeprowadzić zgodnie z postanowieniami niniejszego OPZ w uzgodnieniu z Zamawiającym, zgodnie z obowiązującymi przepisami, zasadami wykonywania projektów teleinformatycznych oraz najlepszymi praktykami w ich realizacji.
  3. Wykonawca jest zobowiązany do realizacji Przedmiotu Zamówienia zgodnie z zasadami i wytycznymi Zamawiającego, zapisami OPZ oraz Wzoru Umowy.
  4. Zamawiający wymaga, aby sprzęt będący przedmiotem dostawy był wyprodukowany nie wcześniej niż 6 miesięcy od dnia dostawy. Oprogramowanie musi być dostarczone i zainstalowane w wersji aktualnej (stabilnej) na dzień jego instalacji. Prace wdrożeniowe muszą być przeprowadzone w taki sposób, aby nie zakłócić normalnej pracy urzędu. Jeżeli podczas prowadzonych prac zaistnieje konieczność rekonfiguracji posiadanych przez Zamawiającego systemów, Wykonawca jest zobowiązany dokonać takich rekonfiguracji na własną odpowiedzialność oraz własny koszt. Zamawiający oczekuje, aby wszystkie wdrożone usługi były realizowane wg najlepszych praktyk zarządzania usługami IT w celu zwiększenia efektywności, skuteczności oraz bezpieczeństwa operacji IT, w szczególności w efektywnym zarządzaniu ryzykiem, reagowaniu na incydenty bezpieczeństwa, a także w zapewnieniu zgodności z przepisami prawnymi i standardami branżowymi.
  5. Ilekroć w niniejszym OPZ Zamawiający użył w opisie oznaczeń norm, aprobat, specyfikacji technicznych i systemów odniesienia, o których mowa w art. 101 ust. 1-3 ustawy PZP należy je rozumieć jako przykładowe. Zamawiający zgodnie z art. 101 ust. 4 ustawy PZP dopuszcza rozwiązanie równoważne opisywanym w treści OPZ. Jeżeli zapisy zawarte w OPZ wskazywałyby w odniesieniu do rozwiązań, materiałów lub urządzeń znaki towarowe lub pochodzenie Zamawiający, zgodnie z art. 101 ust. 4 ustawy PZP dopuszcza składanie ofert na rozwiązania równoważne. Wszelkie „produkty” pochodzące od konkretnych producentów określają minimalne parametry jakościowe i cechy użytkowe, jakim musi odpowiadać produkt, aby spełnić wymagania stawiane przez Zamawiającego, stanowią wyłącznie wzorzec jakościowy przedmiotu zamówienia. Poprzez zapis dotyczący minimalnych wymagań parametrów jakościowych Zamawiający rozumie wymagania materiałów, sprzętu i urządzeń zawarte w ogólnie dostępnych źródłach, katalogach, stronach internetowych producentów. Operowanie przykładowymi nazwami producenta ma jedynie na celu doprecyzowanie poziomu oczekiwań Zamawiającego w stosunku do określonego rozwiązania. Tak więc posługiwanie się nazwami producentów /produktów/ ma wyłącznie charakter przykładowy. Zamawiający, przy opisie przedmiotu zamówienia, wskazując oznaczenie konkretnego producenta (dostawcy) lub konkretny produkt, dopuszcza jednocześnie produkty równoważne o parametrach jakościowych i cechach użytkowych, co najmniej na poziomie parametrów wskazanego produktu, uznając tym samym każdy produkt o wskazanych parametrach lub lepszych. W takiej sytuacji Zamawiający wymaga złożenia stosownych dokumentów, wykazujących spełnienie przez produkty równoważne ww. parametrów i cech.

1. **Termin realizacji Przedmiotu Zamówienia**

Zamawiający wymaga wykonania przedmiotu zamówienia **w terminie 6 miesięcy**  od daty zawarcia umowy w ramach III etapów:

Etap I – do 2 miesięcy od daty zawarcia umowy [kryterium oceny ofert]

Etap II – do 4 miesięcy od daty zawarcia umowy

Etap III – do 6 miesięcy od daty zawarcia umowy

* 1. **Organizacja wdrożenia** 
     1. Założenia podstawowe:
        1. Przedmiot Zamówienia będzie realizowany w oparciu o zdefiniowany uprzednio przez Wykonawcę i zaakceptowany Harmonogram rzeczowo-finansowy, który musi być uzgodniony i zaakceptowany przez Zamawiającego oraz odpowiednio utrzymywany w toku realizacji Przedmiotu Zamówienia. Wykonawca musi przedstawić Harmonogram w terminie 14 dni od daty podpisania umowy.
        2. Wykonawca w Harmonogramie wdrożenia musi w szczególności uwzględnić podział na zadania takie jak: projektowanie, dostawy, usługi instalacji/konfiguracji, testowanie, wdrożenie i odbiory.
        3. Wykonawca umożliwi Zamawiającemu udział we wszystkich realizowanych przez niego pracach w ramach realizacji Przedmiotu Zamówienia (m.in. w czasie projektowania, dostawach, instalacji/budowie, konfiguracji, wdrożeniu i testowaniu).

Wykonawca zobowiązany jest do udziału w cyklicznych spotkaniach, mających na celu przegląd prac w siedzibie Zamawiającego lub w trybie zdalnym, z wykorzystaniem narzędzi komunikacji elektronicznej, które zapewni Wykonawca.

* + - 1. Wykonawca zobowiązany jest przeprowadzić prace wdrożeniowe przedmiotu zamówienia w dokładnych terminach i godzinach uzgodnionych z Zamawiającym.
      2. Wdrożenie będzie realizowane w ramach powołanych do tego celu struktur organizacyjnych po stronie Wykonawcy.
      3. W ramach wdrożenia Wykonawca musi przygotować informacje na temat struktury organizacyjnej Zespołu Wykonawcy zajmującej się realizacją przedmiotu zamówienia, w ramach której muszą zostać powołane minimum następujące role:

1. Kierownik Projektu ze strony Wykonawcy,
2. Zespół Wdrożeniowy ze strony Wykonawcy.
   * + 1. Wdrożenie, z zastrzeżeniami wskazanymi poniżej muszą realizować osoby wymienione w ofercie Wykonawcy, przy czym:
3. Osoby Zespołu Wykonawcy muszą być dyspozycyjne w trakcie wykonywania prac,
4. Wykonawca musi przekazać Zamawiającemu wykaz numerów telefonów kontaktowych do kluczowych osób biorących udział w realizacji Przedmiotu Zamówienia po stronie Wykonawcy.
   1. **Przygotowanie Dokumentacji** 
      1. W ramach realizowanych prac Wykonawca musi opracować dla Zamawiającego Dokumentację Przedmiotu Zamówienia (zwaną dalej Dokumentacją), która składa się z nw. zakresów:
         1. Dokumentacja musi zawierać bazowe zapisy opisujące budowane rozwiązania oraz sposób organizacji prac i wdrożenia. Na podstawie zapisów w Dokumentacji będą prowadzone i odbierane poszczególne etapy realizowane w ramach przedmiotu zamówienia. Dokumenty te wraz ze SWZ z załącznikami będą stanowiły podstawę do weryfikacji wdrożenia w trakcie odbiorów.
         2. Dokumentacja podlega uzgadnianiu i akceptacji Zamawiającego. Akceptacja Harmonogramu wdrożenia i Dokumentacji warunkuje rozpoczęcie prac Wykonawcy.
   2. **Analiza Przedwdrożeniowa**
      1. Analiza Przedwdrożeniowa obejmuje wszystkie czynności do wykonania przez Wykonawcę mające na celu analizę oraz wdrożenie środowiska informatycznego Zamawiającego. Dokumentacja analizy przedwdrożeniowej musi zawierać w szczególności:

|  |  |
| --- | --- |
| minimalna ZAWARTOŚĆ DOKUMENTACJI ANALIZY PRZEDWDROŻENIOWEJ | |
| 1 | Wymagane dane zarządcze |
| a | plan i sposób komunikacji Stron |
| b | harmonogram wdrożenia |
| 2 | Wymagane dane dotyczące systemów cyberbezpieczeństwa |
| a | analiza wymagań przedmiotu zamówienia zawierająca opis sposobu realizacji wymagań, sposób testowania i odbioru |
| b | Dla każdego systemu cyberbezpieczeństwa Wykonawca opracuje:  − Architekturę rozwiązania  − Wersję oprogramowania  − Konfigurację  − Zastosowane licencje/subskrypcje |
| 3 | Procedura testowania – scenariusze testowe dla wdrażanych systemów |
| 4 | Opis instalacji i wdrożenia oprogramowania |

1. **Dokumentacja Powykonawcza** 
   1. Warunkiem dokonania Odbioru Końcowego jest dostarczenie przez Wykonawcę Dokumentacji Powykonawczej obejmującej dokumentację użytkową i techniczną. Dokumentacja Powykonawcza musi być dostarczona w języku polskim, w wersji elektronicznej oraz w wersji elektronicznej w formacie edytowalnym.
   2. W dokumentacji muszą być zawarte opisy wszelkich cech, właściwości i funkcjonalności pozwalających na poprawną z punktu widzenia technicznego eksploatację rozwiązań.
   3. W szczególności dokumentacja ta musi zawierać:
2. Schemat infrastruktury i architekturę rozwiązania
3. Zasady licencjonowania dostarczonych elementów.
4. Konfigurację sprzętową i logiczną elementów infrastruktury dla wdrożonych systemów.
5. Procedury uruchamiania, zatrzymywania wdrożonych systemów oraz elementów infrastruktury.
6. Procedury konfiguracji kont w dostarczonych systemach.
7. Procedury awaryjne umożliwiające dostęp do infrastruktury w przypadku awarii.
8. Procedury wykonywania odtworzenia wdrożonych systemów z kopii zapasowej.
9. Procedury opisujące standardowe działania administracyjne.
10. Procedury odzyskania wdrożonych systemów po awarii.
11. Wytyczne (dobre praktyki) dla administratorów.
12. **Odbiór Etapu/Końcowy** 
    1. Odbiory Etapów będą się odbywać po zakończeniu określonych prac danego Etapu.
    2. Odbiór końcowy przedmiotu zamówienia ma na celu potwierdzenie wykonania wszystkich zadań wynikających z Umowy, w tym odebrania wszystkich Etapów oraz dostarczenia wymaganej zamówieniem Dokumentacji.
    3. Odbiory będą odbywać się zgodnie z zapisami w Umowie
13. **Testy** 
    1. W ramach odbioru przedmiotu zamówienia muszą zostać przeprowadzone testy. Celem testów jest weryfikacja przez Zamawiającego czy wszystkie prace wykonane w trakcie realizacji przedmiotu zamówienia zostały wykonane prawidłowo i zgodnie z założeniami funkcjonalnymi i jakościowymi. Testy będą przeprowadzane przez Wykonawcę przy współudziale Zamawiającego.
    2. Zamawiający ma prawo do weryfikacji należytego wykonania Umowy dowolną metodą, w tym także z wykorzystaniem opinii zewnętrznego audytora. W szczególności uzgodnienie określonych scenariuszy testowych nie wyklucza prawa do weryfikacji prac innymi testami i scenariuszami.
    3. W przypadku zidentyfikowania Błędów lub Wad Wykonawca jest zobowiązany do ich poprawy przed Odbiorem Końcowym przedmiotu zamówienia.
    4. Zamawiający wymaga, aby Wykonawca przeprowadził testy odbiorcze z zakresu:
14. Uruchamianie i zatrzymywanie wdrożonych systemów
15. Weryfikacja wdrożonych systemów zgodnie ze scenariuszami opisanymi w dokumentacji.
16. Weryfikacja poprawności działania procedur.
17. Symulację awarii wdrożonych systemów.
18. **Dodatkowe zobowiązania Wykonawcy** 
    1. Wykonanie przedmiotu zamówienia z efektywnością oraz zgodnie z praktyką i wiedzą zawodową.
    2. Dokonanie z Zamawiającym wszelkich koniecznych ustaleń mogących wpływać na zakres i sposób realizacji Przedmiotu Zamówienia oraz ciągła współpraca z Zamawiającymi na każdym etapie realizacji.
    3. Stosowanie się do wytycznych i polityk bezpieczeństwa informacji obowiązujących u Zamawiającego.
    4. Udzielanie na każde żądanie Zamawiającego pełnej informacji na temat stanu realizacji Przedmiotu Zamówienia.
    5. Współdziałanie z osobami wskazanymi przez Zamawiającego.

**Rozdział II. Szczegółowy opis przedmiotu zamówienia**

* 1. **Dostawa, wdrożenie, instalacja serwera I, instruktaż z zakresu administracji i bieżącej obsługi dostarczonego sprzętu**

|  |  |
| --- | --- |
| parametr | charakterystyka [wymagania minimalne] |
| obudowa | Obudowa Rack o wysokości max 1U z możliwością instalacji min. 8 dysków 2.5” |
| płyta główna | Płyta główna z możliwością zainstalowania procesora.  Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.  Płyta powinna obsługiwać do min. 128GB, na płycie głównej powinno znajdować się min. 4 sloty przeznaczone dla pamięci |
| chipset | Dedykowany przez producenta procesora do pracy w serwerach jednoprocesorowych |
| procesor | Jeden procesor 8-rdzeniowy, min. 3.2GHz, umożliwiający osiągnięcie wyniku min. 95 w teście SPECrate2017\_int\_base dostępnym na stronie www.spec.org w konfiguracji jednoprocesorowej |
| pamięć ram | Min. 2x16GB pamięci RAM o częstotliwości pracy min. 4800MT/s |
| karta graficzna | Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1920x1200 |
| wbudowane porty | min. 4 porty USB w tym 1 port USB 3.0 z tyłu obudowy, 1 port VGA na tylnym panelu, 1 port RS232 |
| interfejsy sieciowe/fc/sas | Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz min. 2 porty 10Gb w standardzie 10GBase-T |
| kontroler raid | Sprzętowy kontroler dyskowy, posiadający możliwość konfiguracji poziomów RAID: 0, 1, 10 |
| dyski twarde | Min. 8x dysk 2,5’’ w konfiguracji 2xSSD SAS 1,92TB  Min. 6x dysk 2,5’’ SAS min 2,4TB |
| diagnostyka | Łatwodostępny panel LCD, umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze |
| zasilacze | Redundantne, o mocy maks. 700W klasy Titanium |
| bezpieczeństwo | Zatrzask górnej pokrywy oraz blokada na ramce panela, zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych  Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.  Moduł TPM 2.0 |
| elementy montażowe | Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych |
| system operacyjny | Licencja na serwerowy system operacyjny musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym lub umożliwiać zainstalowanie czterech instancji wirtualnych tego serwerowego systemu operacyjnego.  Licencja musi zostać tak dobrana aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze. Wymaga się, aby oferowane licencje umożliwiały korzystanie min. 80 użytkownikom.  Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.   1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym. 2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny. 3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych. 4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. 5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. 9. Wbudowane wsparcie instalacji i pracy na wolumenach, które: 10. pozwalają na zmianę rozmiaru w czasie pracy systemu, 11. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, 12. umożliwiają kompresję „w locie” dla wybranych plików i/lub folderów, 13. umożliwiają zdefiniowanie list kontroli dostępu (ACL). 14. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 15. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 16. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET 17. Możliwość dystrybucji ruchu sieciowego http pomiędzy kilka serwerów. 18. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 19. Dostępne dwa rodzaje graficznego interfejsu użytkownika: 20. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, 21. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych. 22. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, 23. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. 24. Mechanizmy logowania w oparciu o: 25. Login i hasło, 26. Karty z certyfikatami (smartcard), 27. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), 28. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.. 29. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 30. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 31. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 32. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). 33. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. 34. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: 35. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, 36. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:  * Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, * Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, * Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. * Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows  1. Zdalna dystrybucja oprogramowania na stacje robocze. 2. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej 3. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:  * Dystrybucję certyfikatów poprzez http * Konsolidację CA dla wielu lasów domeny, * Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, * Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.  1. Szyfrowanie plików i folderów. 2. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). 3. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów. 4. Serwis udostępniania stron WWW. 5. Wsparcie dla protokołu IP w wersji 6 (Ipv6), 6. Wsparcie dla algorytmów Suite B (RFC 4869), 7. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, 8. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:  * Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, * Obsługi ramek typu jumbo frames dla maszyn wirtualnych. * Obsługi 4-KB sektorów dysków * Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra * Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API. * Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. Trunk mode)  1. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. 2. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath). 3. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. 4. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. 5. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. |
| karta zarządzania | Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:   * zdalny dostęp do graficznego interfejsu Web karty zarządzającej; * zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); * szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; * możliwość podmontowania zdalnych wirtualnych napędów; * wirtualną konsolę z dostępem do myszy, klawiatury; * wsparcie dla IPv6; * wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; * możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; * możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; * integracja z Active Directory; * możliwość obsługi przez dwóch administratorów jednocześnie; * wsparcie dla dynamic DNS; * wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. * możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera * możliwość zarządzania serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera |
| certyfikaty | * Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 * Serwer musi posiadać deklarację CE. * musi zawierać informacje dotyczące ponownego użycia i recyklingu - nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC.   Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej [www.epeat.net](http://www.epeat.net/) potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku - **Wykonawca złoży dokument potwierdzający spełnianie wymogu.**   * Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022. |
| dokumentacja użytkownika | Zamawiający wymaga dokumentacji w języku polskim lub angielskim.  Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |
| warunki gwarancji | * Gwarancja producenta: min. 2 lata * Możliwość rozszerzenia gwarancji przez producenta do 7 lat * Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. * Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego. * Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych. * Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania. * Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. * Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera. * Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii. * Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych. * **Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia**, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. * Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – **dokumenty potwierdzające należy załączyć do oferty.** * **Wymagane dołączenie do oferty oświadczenia Producenta** potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. |
| konfiguracja | Instalacja urządzeń w istniejącej infrastrukturze Zamawiającego w uzgodnieniu z Zespołem Informatyki. |

* 1. **Dostawa, wdrożenie, instalacja serwera II, instruktaż z zakresu administracji i bieżącej obsługi dostarczonego sprzętu**

|  |  |
| --- | --- |
| parametr | charakterystyka [wymagania minimalne] |
| obudowa | Obudowa Rack o wysokości max 1U z możliwością instalacji min. 8 dysków 2.5”  Obudowa wyposażona w panel LCD umieszczony na froncie obudowy  Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI. |
| płyta główna | Płyta główna z możliwością zainstalowania do dwóch procesorów.  Obsługa procesorów 32 rdzeniowych.  Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.  Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci.  Płyta główna powinna obsługiwać do 1TB pamięci RAM. |
| chipset | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych |
| procesor | Dwa procesory 8-rdzeniowe, min. 2.9GHz, umożliwiające osiągnięcie wyniku min. 176 w teście SPECrate2017\_int\_base, dla oferowanego serwera, dostępnym na stronie www.spec.org w konfiguracji dwuprocesorowej |
| pamięć ram | Minimum 64GB min. 4800MT/s, |
|  | Demand Scrubing,  Patrol Scrubing,  Permanent Fault Detection |
| gniazda pci | minimum trzy sloty PCIe |
| wbudowane porty | 4 x USB z czego nie mniej niż 1x USB 3.0, 2x VGA |
| interfejsy sieciowe/fc/sas | Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) |
| kontroler raid | Sprzętowy kontroler dyskowy, posiadający min. 8GB nieulotnej pamięci cache,  Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60.  Wsparcie dla dysków samoszyfrujących |
| dyski twarde | 2x dysk SSD SAS MU o pojemności min. 1.6TB, Hot-Plug.  6x dysk SAS o pojemności min. 2.4TB, Hot-Plug.  Zainstalowane dwa dyski M.2 NVMe SSDs o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1. |
| karta graficzna | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200 |
| zasilacze | Redundantne, Hot-Plug min. 1100W klasy Titanium |
| bezpieczeństwo | Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych.  Możliwość wyłączenia w BIOS funkcji przycisku zasilania.  BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła  Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.  Moduł TPM 2.0  Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera  Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem |
| elementy montażowe | Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych  Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych |
| system operacyjny | Licencja na serwerowy system operacyjny musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym lub umożliwiać zainstalowanie czterech instancji wirtualnych tego serwerowego systemu operacyjnego.  Licencja musi zostać tak dobrana aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze. Wymaga się, aby oferowane licencje umożliwiały korzystanie min. 80 użytkownikom.  Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.   1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym. 2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny. 3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych. 4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. 5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. 9. Wbudowane wsparcie instalacji i pracy na wolumenach, które: 10. pozwalają na zmianę rozmiaru w czasie pracy systemu, 11. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, 12. umożliwiają kompresję „w locie” dla wybranych plików i/lub folderów, 13. umożliwiają zdefiniowanie list kontroli dostępu (ACL). 14. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 15. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 16. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET 17. Możliwość dystrybucji ruchu sieciowego http pomiędzy kilka serwerów. 18. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 19. Dostępne dwa rodzaje graficznego interfejsu użytkownika: 20. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, 21. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych. 22. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, 23. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. 24. Mechanizmy logowania w oparciu o: 25. Login i hasło, 26. Karty z certyfikatami (smartcard), 27. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), 28. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych. 29. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 30. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 31. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 32. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). 33. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. 34. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: 35. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, 36. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:  * Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, * Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, * Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. * Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows  1. Zdalna dystrybucja oprogramowania na stacje robocze. 2. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej 3. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:  * Dystrybucję certyfikatów poprzez http * Konsolidację CA dla wielu lasów domeny, * Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, * Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.  1. Szyfrowanie plików i folderów. 2. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). 3. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów. 4. Serwis udostępniania stron WWW. 5. Wsparcie dla protokołu IP w wersji 6 (Ipv6), 6. Wsparcie dla algorytmów Suite B (RFC 4869), 7. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, 8. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:  * Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, * Obsługi ramek typu jumbo frames dla maszyn wirtualnych. * Obsługi 4-KB sektorów dysków * Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra * Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API. * Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. Trunk mode)  1. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. 2. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath). 3. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. 4. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. 5. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. |
| OPROGRAMOWANIE | Oprogramowanie do archiwizacji poczty elektronicznej dla min. 250 kont pocztowych. Oprogramowanie ma zapewnić bezpieczne, wydajne i zgodne z przepisami archiwizowanie wiadomości e-mail, umożliwiając łatwy dostęp, zarządzanie i przeszukiwanie zarchiwizowanych wiadomości. Oprogramowanie powinno zapewniać:  Archiwizacja poczty:   * Archiwizacja wiadomości e-mail z różnych źródeł (serwery pocztowe, skrzynki użytkowników, pliki PST). * Wsparcie dla najpopularniejszych serwerów pocztowych, takich jak Microsoft Exchange, Office 365, Google Workspace, oraz serwerów IMAP/POP3. * Automatyczne harmonogramy archiwizacji.   Bezpieczeństwo:   * Szyfrowanie zarchiwizowanych danych. * Zabezpieczenia przed nieautoryzowanym dostępem do zarchiwizowanych wiadomości.   Przeszukiwanie i odzyskiwanie:   * Zaawansowane funkcje wyszukiwania pełnotekstowego. * Szybkie odzyskiwanie pojedynczych wiadomości lub całych skrzynek pocztowych. * Opcja przywracania wiadomości bezpośrednio do skrzynek użytkowników.   Zarządzanie użytkownikami i administracja:   * Łatwe zarządzanie użytkownikami i ich uprawnieniami. * Raportowanie i monitorowanie działania systemu. * Integracja z Active Directory. |
| karta zarządzania | Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:   * zdalny dostęp do graficznego interfejsu Web karty zarządzającej; * zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); * szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; * możliwość podmontowania zdalnych wirtualnych napędów; * wirtualną konsolę z dostępem do myszy, klawiatury; * wsparcie dla IPv6; * wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; * możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; * możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; * integracja z Active Directory; * możliwość obsługi przez dwóch administratorów jednocześnie; * wsparcie dla dynamic DNS; * wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. * możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera * możliwość zarządzania serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera |
| certyfikaty | * Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 * Serwer musi posiadać deklarację CE. * musi zawierać informacje dotyczące ponownego użycia i recyklingu - nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC.   Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej [www.epeat.net](http://www.epeat.net/) potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku - **Wykonawca złoży dokument potwierdzający spełnianie wymogu.**   * Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022. |
| dokumentacja użytkownika | Zamawiający wymaga dokumentacji w języku polskim lub angielskim.  Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |
| warunki gwarancji | * Gwarancja producenta: min. 2 lata * Możliwość rozszerzenia gwarancji przez producenta do 7 lat * Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. * Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego. * Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych. * Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania. * Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. * Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera. * Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii. * Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych. * **Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia**, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. * Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – **dokumenty potwierdzające należy załączyć do oferty.** * **Wymagane dołączenie do oferty oświadczenia Producenta** potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. |
| konfiguracja | Instalacja urządzeń w istniejącej infrastrukturze Zamawiającego w uzgodnieniu z Zespołem Informatyki. |

* 1. **Dostawa, wdrożenie systemu do ochrony brzegu sieci klasy UTM, instruktaż z zakresu administracji i bieżącej obsługi dostarczonego systemu UTM**

|  |  |
| --- | --- |
| parametr | charakterystyka [wymagania minimalne] |
| obsługa sieci | Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP |
| zapora korporacyjna | Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.  Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.  Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).  Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.  Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia.  Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac.  Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall.  Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.  Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.  Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego) |
| ips | System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.  Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.  Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.  Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS.  Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia.  Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS.  Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP.  Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.  Po zakupie stosownej licencji moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose & SV).  Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.  Urządzenie ma posiadać moduł wykrywania typu i wersji oprogramowania sieciowego, którego ruch jest filtrowany przez urządzenie. Moduł musi działać na urządzeniu. Nie dopuszcza się stosowania rozwiązania z agentem instalowanym na komputerach w sieci.  Powyższy moduł ma nie tylko wykrywać oprogramowanie ale również wykrywać i informować o lukach i podatnościach występujących w wykrytym oprogramowaniu |
| kształtowanie pasma | Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.  Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.  Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring).  Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch |
| ochrona antywirusowa | Urządzenie ma umożliwiać zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania).  Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji.  Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.  Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji.  Urządzenie ma być dostarczone wraz z komercyjnym, europejskim skanerem Antywirusowym |
| ochrona antyspam | Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).  Ochrona antyspam ma działać w oparciu o:   1. białe/czarne listy, 2. DNS RBL, 3. Skaner heurystyczny.   W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.  Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin |
| wirtualne sieci prywatne (vpn) | Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).  Urządzenie ma wspierać co najmniej następujące typy sieci VPN:   1. PPTP VPN, 2. IPSec VPN, 3. SSL VPN.   SSL VPN ma działać co najmniej w trybach tunelu i portalu.  Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.  Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal)  Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).  Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf.  Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based |
| filtr dostępu do stron www | Urządzenie ma posiadać wbudowany filtr URL.  Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych.  Administrator ma mieć możliwość dodawania własnych kategorii URL.  Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej:  a.blokowanie dostępu do adresu URL,  b.zezwolenie na dostęp do adresu URL,  c.blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.  Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.  Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.  Filtr URL musi uwzględniać komunikację po protokole HTTPS.  Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.  Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.  Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch |
| uwierzytelnianie | Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o:   1. lokalną bazę użytkowników (wewnętrzny LDAP), 2. zewnętrzną bazę użytkowników (zewnętrzny LDAP), 3. usługę katalogową Microsoft Active Directory.   Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.  Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły:   1. SSL, 2. Radius, 3. Kerberos.   Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.  Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.  Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.  Rozwiązanie musi mieć możliwość transparentnego uwierzytelniania użytkowników w ramach infrastruktury VDI (Virtual Desktop Infrastructure) poprzez dedykowanego agenta. Metoda ta musi wspierać co najmniej technologie Citrix Virtual Apps i Microsoft Remote Desktop Services (RDS).  Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP).  Wbudowany moduł 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH. |
| ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP) | Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).  Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:  a.równoważenie względem adresu źródłowego,  b.równoważenie względem połączenia.  Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.  Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover).  Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza.  W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów).  Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP |
| ROUTING (TRASOWANIE) | Urządzenie ma umożliwiać statyczne trasowanie pakietów.  Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.  Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).  Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP. |
| ADMINISTRACJA URZĄDZENIEM | Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.  Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.  Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.  Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.  Urządzenie musi oferować możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.  Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH)  Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.  Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.  Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup.  Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.  Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła.  Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora ( script recording ).  System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services).  Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników.  Urządzenie ma umożliwiać zapisywanie logów na wbudowanym dysku.  Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).  Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.  Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie:  a.manualnego eksportu do pliku w dowolnym momencie czasu,  b.automatycznego eksportu do serwerów producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu  Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzącego bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora.  Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.  Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego. |
| RAPORTOWANIE | Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.  System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.  System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.  System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów.  System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.  System raportowania ma umożliwiać eksport wyników raportu do formatu CSV.  Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta.  Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3.  Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH). |
| POZOSTAŁE USŁUGI I FUNKCJE | Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP.  Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.  Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).  Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.  Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny).  Urządzenie ma posiadać usługę DNS Proxy.  Urządzenie ma posiadać wsparcie dla Spanning-tree protocol (RSTP/MSTP).  Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN.  Urządzenie musi mieć zaimplementowane Open API  Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie. |
| GWARANCJA I SERWIS | Urządzenie ma być objęte min. 24-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa (nie dłużej niż do 30.06.2026r.).  W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal. |
| PARAMETRY SPRZĘTOWE | Urządzenie ma być wyposażone w dysk SSD o pojemności co najmniej 200 GB.  Urządzenie wyposażone jest w redundantne zasilanie z sygnalizacją pracy poszczególnych zasilaczy.  Liczba portów Ethernet 2,5Gbps – min. 8 z możliwością rozszerzenia do 16.  Liczba portów światłowodowych 1Gbps – min. 2 z możliwością rozszerzenia do 10.  Urządzenie ma pozwalać na instalację modułu rozszerzeń z poniższej listy:  a.Moduł z 8 interfejsami miedzianymi 2,5Gbps  b.Moduł z 4 interfejsami miedzianymi 10Gbps.  c.Moduł z 4 interfejsami światłowodowymi 1Gbps.  d.Moduł z 8 interfejsami światłowodowymi 1Gbps.  Moduł z 4 interfejsami światłowodowymi 10Gbps.  Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.  Urządzenie ma być wyposażone w min. 2, różniące się typem, porty konsolowe. Przynajmniej jeden port konsolowy ma być typu RJ45.  Przepustowość Firewall (1518 bajtów UDP) – minimum 10Gbps.  Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 5Gbps.  Przepustowość filtrowania Antywirusowego – minimum 1.3 Gbps.  Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 2.5Gbps.  Maksymalna liczba tuneli VPN IPSec – minimum 1000.  Maksymalna liczba tuneli typu SSL VPN (tryb tunelu) – minimum 150.  Maksymalna liczba tuneli typu SSL VPN (tryb portalu) – minimum 150.  Obsługa interfejsów 802.11q (VLAN) – minimum 256.  Liczba równoczesnych sesji – minimum 600 000 i nie mniej niż 30 000 nowych sesji/sekundę.  Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive.  Urządzenie nie ma limitu na liczbę użytkowników.  Liczba reguł filtrowania – minimum 16 384.  Liczba tras statycznego routingu – minimum 5 120.  Liczba tras dynamicznego routingu – minimum 10 000.  Możliwość instalacji w szafie RACK 19”, wysokość urządzenia 1U.  Urządzenie musi być wyposażone w moduł TPM. |
| konfiguracja | Instalacja urządzeń w istniejącej infrastrukturze Zamawiającego w uzgodnieniu z Zespołem Informatyki. |
|  |  |

* 1. **Dostawa, wdrożenie, instalacja Biblioteki taśmowej, instruktaż z zakresu administracji i bieżącej obsługi dostarczonego systemu**

|  |  |
| --- | --- |
| parametr | charakterystyka [wymagania minimalne] |
| obudowa i pojemość | Wysokość maksymalnie 1U do instalacji w szafie Rack, co najmniej 9 slotów przeznaczonych na zestaw taśm |
| połączenie | Co najmniej 1 port SAS o przepustowości co najmniej 6Gb/s w standardzie umożliwiającym podłączenie serwerów  Co najmniej 1 port 1GB RJ-45 |
| napęd | Wyposażony w co najmniej 1 sztukę napędu SAS LTO 8., kabel SAS umożliwiający podłączenie biblioteki do serwera o dł. min. 2m, 5x taśma LTO8 |
| gwarancja | Min. 2 lata gwarancji producenta  Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji.  Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego.  Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych.  Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania.  Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.  Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji urządzenia.  Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych.  Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – **dokumenty potwierdzające należy załączyć do oferty.**  **Wymagane dołączenie do oferty oświadczenia Producenta** potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. |
| konfiguracja | Instalacja urządzeń w istniejącej infrastrukturze Zamawiającego w uzgodnieniu z Zespołem Informatyki. |

* 1. **Dostawa, wdrożenie sieciowego serwera plikowego typu NAS, instruktaż z zakresu administracji i bieżącej obsługi dostarczonego sprzętu**

|  |  |
| --- | --- |
| parametr | charakterystyka [wymagania minimalne] |
| procesor | Procesor osiągający w teście Passmark CPU Mark średni wynik przynajmniej 9800 punktów.  Do oferty należy dołączyć wydruk ze strony: www.cpubenchmark.net/high\_end\_cpus.html |
| kontroler | Min. 2 moduły kontrolera o architekturze active-active |
| pamięć | Min. 8 GB (na kontroler)  Maksymalna pojemność pamięci: min. 32 GB (na kontroler) |
| pamięć masowa | Kieszeń/kieszenie na dyski min. 12 szt.  Obsługiwane dyski twarde:  - 2,5-calowy dwuportowy dysk SSD SAS  - 3,5-calowy dwuportowy dysk HDD SAS  Dysk z możliwością wymiany podczas pracy (hot-swap) |
| zainstalowane dyski | Zainstalowane min. 12 szt. dysków producenta urządzenia o parametrach:  - pojemność: min. 12TB każdy (łącznie min. 144TB)  - Interfejs: SAS  - prędkość obrotowa min. 7200 obr/min.  - Rozmiar buforu min. 256 MB |
| porty zewnętrzne | Port LAN RJ-45 1GbE: min. 2 szt. (na kontroler)  Port LAN RJ-45 10GbE: min. 1 szt. (na kontroler)  Port SFP+ 10Gb: min. 2 szt. (na kontroler) |
| zasilanie | Zasilacz max. 550 W |
| inne | Wykonawca dostarczy zestaw szyn do montażu w szafie rack |
| gwarancja | Gwarancja producenta min. 24 miesiące |
| konfiguracja | Instalacja urządzeń w istniejącej infrastrukturze Zamawiającego w uzgodnieniu z Zespołem Informatyki. |

* 1. **Dostawa, wdrożenie Oprogramowania do przeciwdziałania wyciekom danych dla 100 użytkowników, instruktaż z zakresu administracji i bieżącej obsługi dostarczonego systemu**

|  |  |
| --- | --- |
|  | charakterystyka [wymagania minimalne] |
|  | 1. Obsługiwane systemy operacyjne: 2. Windows 10 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi 3. Windows 11 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi 4. MacOS 12 lub nowszy. 5. Serwer administracyjny musi obsługiwać instalację na systemach: a. Windows Server 2016 (64-bit) i nowszych. 6. Serwer administracyjny musi obsługiwać bazy danych: 7. MS SQL Server 2016 lub nowsze, 8. MS SQL Express, 9. AzureSQL S3 lub nowsze. 10. Pomoc i dokumentacja programu dostępne w języku angielskim. 11. Konsola administracyjna i komunikaty klienta muszą być w języku polskim. 12. Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta. 13. Serwer administracyjny musi umożliwiać instalację/dezinstalację zdalnego klienta na stacjach roboczych. 14. Reguły DLP muszą być egzekwowane nawet przy braku połączenia między klientem a serwerem zarządzającym. 15. Brak połączenia klienta z serwerem zarządzającym musi umożliwiać lokalne przechowywanie informacji i zebranych danych do czasu ponownego połączenia. 16. Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsoli. 17. Administrator musi mieć możliwość konfiguracji automatycznej konserwacji dla bazy danych, usuwając najstarsze informacje, gdy rozmiar bazy osiągnie skonfigurowany limit. 18. Serwer administracyjny musi automatycznie pobierać aktualizacje definicji kategoryzowania stron internetowych, aplikacji i rozszerzeń plików, z opcją wyłączenia automatycznego pobierania. 19. Administrator musi mieć możliwość aby tworzyć, usuwać i konta administratorów w konsoli programu. 20. Administrator musi mieć możliwość przypisywania i odbierania uprawnień do wybranych modułów programu, podzielonych na ustawienia (konfiguracja modułu) i logi (wyświetlanie logów modułu). 21. Serwer musi synchronizować użytkowników i stacje robocze z domeną Active Directory. 22. System musi rejestrować zdarzenia aktywności stacji roboczej, takie jak logowanie, wylogowanie, włączenie, wyłączenie, blokada, odblokowanie i przejście w stan bezczynności. 23. Administrator musi móc wymusić synchronizację ustawień i logów między stacją roboczą a serwerem w czasie rzeczywistym. 24. Serwer administracyjny musi umożliwiać ustawienie powiadomień dla użytkownika końcowego w przypadku złamania reguł związanych z ochroną DLP, z możliwością dostosowania grafiki, adresu e-mail i odnośnika do polityki bezpieczeństwa. 25. Administrator musi mieć możliwość wykonać audyt stacji roboczych/użytkowników w oparciu o różne czynności, takie jak uruchomione aplikacje, podłączone urządzenia, odwiedzane strony internetowe, wydrukowane dokumenty, wysyłane i odebrane wiadomości e-mail oraz czynności na plikach. 26. Administrator musi mieć możliwość tworzenia własnych kategorii dla stron internetowych, aplikacji i typów plików. 27. Administrator musi mieć możliwość filtrowania i sortowania zebranych danych. 28. Serwer musi posiadać możliwość wysyłania alertów, przynajmniej za pośrednictwem wiadomości email. 29. Dashboardy muszą być generowane na podstawie wskazanych stacji roboczych, użytkowników lub grup w określonym przedziale czasu. 30. Serwer administracyjny musi posiadać wbudowany serwer SMTP dostarczony przez producenta oprogramowania. 31. Serwer administracyjny musi umożliwiać wykonywanie zadań kategoryzacji plików, zarówno istniejących na stacjach roboczych i zasobach sieciowych, jak i nowo powstałych na bazie już skategoryzowanych plików. 32. Serwer administracyjny musi mieć możliwość kategoryzacji plików wrażliwych na podstawie aplikacji, lokalizacji, adresu URL, formatu pliku i zawartości pliku. 33. Administrator musi mieć możliwość wyszukiwania danych osobowych na zasobach zarówno lokalnych, jak i sieciowych. 34. Dla plików skategoryzowanych, wymagana jest możliwość tworzenia reguł dotyczących blokowania i zezwalania na różne operacje, takie jak zapisywanie, przenoszenie, drukowanie, wysyłanie pocztą, wysyłanie do chmury, przesyłanie komunikatorami itp. 35. Serwer administracyjny musi umożliwiać wyszukiwanie i ochronę plików w oparciu o różne kryteria, takie jak numery kart kredytowych, numer PESEL, numer dowodu osobistego, numer paszportu, wyrażenia regularne, określone ciągi znaków i numer IBAN. 36. Weryfikacja zawartości pliku musi odbywać się w czasie rzeczywistym. 37. Serwer administracyjny musi pozwalać na eksport logów do rozwiązania SIEM. 38. Konsola musi umożliwiać konfigurację/zmianę domyślnego serwera SMTP. 39. Konsola webowa musi pozwalać na weryfikację wersji zainstalowanego oprogramowania klienta, a także umożliwia aktualizację do nowej wersji lub dezaktywację tego oprogramowania. 40. System musi ochraniać pocztę e-mail Microsoft 365, sprawdzając każdą wiadomość e-mail wysyłaną przez użytkowników Microsoft 365. 41. System musi ochraniać pliki w Microsoft 365, kontrolując aktywność plików w Microsoft SharePoint, Microsoft OneDrive dla Firm i Microsoft Teams. 42. System musi wykorzystywać mechanizm OCR (optical character recognition), aby wykrywać poufne treści w obrazach, zdjęciach i zeskanowanych dokumentach 43. Licencja wieczysta dla min. 100 użytkowników z wsparciem producenta na min. 2 lata |

* 1. **Dostawa, wdrożenie, instalacja 2 przełączników sieciowych, instruktaż z zakresu administracji i bieżącej obsługi dostarczonego sprzętu**

|  |  |
| --- | --- |
| parametr | charakterystyka [wymagania minimalne] |
| opis | * Ilość portów min. 24 x SFP+ 10GB (zainstalowanych min. 12 szt. kompatybilnych wkładek SFP+ 10GB), min. 4 x SFP28 10/25G * Tablica MAC min. 16K * Tablica min. 4K ARP/ 512 NDP * Bufor min. 32Mb * MTBF min. 778741 godzin * Wydajność min. 505 Mp/s * Przepustowość min. 680 Gb/s * min. 1xPort USB-C * min. 1xPort zarządzania Out-of-band; * Web GUI * HTTPs * CLI * Telnet * SSH * SNMP * MIB RSPAN * Radius * TACACS+ * DiffServ * Możliwość limitowania przepustowości do 1 Kbps w oparciu o harmonogram * Wymaga się aby interfejs web miał możliwość wykonywania poleceń tekstowych CLI bez potrzeby tworzenia oddzielnego połączenia Telnet lub SSH. * IPv4/IPv6 Multicast filtering * IGMPv3 MLDv2 Snooping * ASM & SSM * IGMPv1,v2 Querier * Policy-based routing (PBR) * LLDP-MED * Spanning Tree * Green Ethernet * STP * MTP * RSTP * EEE (802.3az) * GVRP/GMRP * Q in Q, * Private VLAN * DOT1X * MAB * Captive Portal * DHCP Snooping * Dynamic ARP * Inspection * IP Source Guard * CPU min ARMv8 1.8Ghz * Min 2GB RAM * Min 512MB Flash * Min ilość obsługiwanych VLAN 4K * DHCP Server min 2K rezerwacji * sFlow * Minimalna ilość przełączników w stosie: 8 * Możliwość łączenia w stos za pomocą interfejsów 25Gb/s * Możliwość łączenia przełączników w stos w konfiguracji: pierścień, podwójny pierścień, mesh * Distributed Link Aggregation (LAGs across the stack) * Min. ilość interfejsów IP 128 * Double VLAN Tagging (QoQ) * Yes * PIM-DM (Multicast Routing - dense mode) * PIM-DM (IPv6) * PIM-SM (Multicast Routing - sparse mode) * PIM-SM (IPv6) * RIPv1 * RIPv2 * OSPFv2 * RFC 2328 * RFC 1583 * OSPFv3 * OSPFv2 min. sąsiadów 400 * OSPFv3 min. sąsiadów 400 * OSPFv3 min. sąsiadów na interfejs 100 * UDLD * LLPF * DHCPv6 Snooping * wysyłanie alertów na email * MMRP * Ilość ACL min. 100 * Ilość reguł na listę min. 1000 na wejściu i min. 500 na wyjściu |
| gwarancja | Gwarancja producenta min. 2 lata realizowana w systemie door-to-door przez serwis producenta. Urządzenie powinno być objęte usługą szybkiej wymiany w wypadku awarii z wysyłką w następnym dniu roboczym po stwierdzeniu awarii przez okres gwarancji. |
| konfiguracja | Instalacja urządzeń w istniejącej infrastrukturze Zamawiającego w uzgodnieniu z Zespołem Informatyki. |

* 1. **Dostawa, wdrożenie, instalacja oprogramowania do wykonywania kopii zapasowych, instruktaż z zakresu administracji i bieżącej obsługi dostarczonego systemu**

|  |  |
| --- | --- |
| parametr | charakterystyka [wymagania minimalne] |
| wymagania ogólne | Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 6.x, 7.x i 8.0 oraz Microsoft Hyper-V 2012, 2012R2, 2016, 2019 i 2022. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej  Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux |
| opis | Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej  Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków  Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji  Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.  Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli.  Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage oraz na innych kompatybilnych z S3 przestrzeniach obiektowych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier.  Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu.  Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania  Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time)  Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu  Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API  Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji  Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji  Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania  Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.  Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej |
| wymagania rpo | Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej  Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.  Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych z dokładnością do pojedynczego datastoru  Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware.  Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.  Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy.  Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)  Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard.  Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.  Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.  Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.  Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO.  Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik  Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)  Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN) |
| wymagania rto | Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware, Hyper-V oraz Nutanix AHV niezależnie od rodzaju storage’u użytego do przechowywania kopii zapasowych.  Dodatkowo dla środowiska vSphere, Hyper-V i Nutanix AHV powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)  Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami  Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre  Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL i Oracle bezpośrednio ze skompresowanego i skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne.  Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków  Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform.  Oprogramowanie musi umożliwić odtworzenie plików/folderów lub ich uprawnień na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików  Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy natywnego API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.  Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell  Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.  Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.  Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA, elementów AD Sites oraz pozwalać na odtworzenie haseł.  Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2013SP1 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego.  Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2008 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur.  Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2013 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku całych witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji.  Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.  Oprogramowanie musi wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux.  Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN  Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle  Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI  Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN |
| ograniczenie ryzyka | Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)  Dla VMware’a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.  Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem  Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32.  Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego |
| agent | Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego  Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych  Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE  Rozwiązanie musi wspierać system operacyjny macOS  Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix  Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą)  Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster  Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów  Rozwiązanie musi wspierać backup podłączonych dysków USB  Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym  Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na zasobach lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire, Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS, bezpośrednio na zasobach obiektowych (w tym chmury)  Rozwiązanie musi wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone  Rozwiązanie musi wspierać kontrolę pasma sieciowego  Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych  Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN  Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft  Rozwiązanie musi wspierać technologię BitLocker  Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania  Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla Microsoft Exchange 2013SP1 i nowszych, Microsoft Active Directory 2008 i nowszych, Microsoft Sharepoint 2013 i nowszych, Microsoft SQL 2008 i nowszych, Oracle 11g i nowszych oraz PostgreSQL 12 i nowszych  Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych  Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL i Oracle poprzez bezpośrednie uruchomienie ich z pliku backupu.  Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do vSphere, Hyper-V, Nutanix AHV, Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform  Rozwiązanie musi wspierać szyfrowanie  Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne  Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego  Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej  Rozwiązanie musi wspierać tworzenie wielu zadań backupowych |
| licencja | Licencja umożliwiająca backup 100 komputerów, 2 serwerów fizycznych oraz 8 serwerów wirtualnych. Wsparcie producenta oprogramowania na okres min. 2 lata. |

* 1. **Dostawa, wdrożenie, instalacja oprogramowania umożliwiającego monitoring usług i systemów użytkowanych przez Zamawiającego wraz z możliwością wysyłania powiadomień e-mail/sms, instruktaż z zakresu administracji i bieżącej obsługi dostarczonego systemu**

Przez wdrożenie systemu monitorowania Zamawiający rozumie dostawę licencji, zaprojektowanie systemu oraz jego uruchomienie, a także przeprowadzenie instruktażu z zakresu administracji i jego obsługi.

System monitorowania ma stanowić narzędzie pozwalające na gromadzenie i analizowanie danych dotyczących różnorodnych zdarzeń związanych z użytkowanymi przez Zamawiającego systemami teleinformatycznymi wraz z powiadamianiem zespołów bezpieczeństwa.

Zaproponowanie rozwiązanie powinno wspierać zespół monitorowania w procesie reakcji na wykryte incydenty. System ma przetwarzać dane zarówno w celu bezpośredniego monitorowania systemów i usług jak i także w celu wsparcia procesu utrzymywania zgodności z regulacjami prawnymi oraz standardami bezpieczeństwa, w szczególności w celu wypełnienia obowiązków wynikających z:

* Ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne,
* Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych,
* Ustawy z dnia 10 listopada 2020 r. o doręczeniach elektronicznych
* Rozporządzenia Ministra Cyfryzacji z dnia 5 października 2016 r. w sprawie zakresu i warunków korzystania z elektronicznej platformy usług administracji publicznej,
* Ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa,
* Ustawy z dnia 5 września 2016 r. o usługach zaufania i identyfikacji elektronicznej,
* Ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną,
* Ustawą z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach,
* Ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych.

|  |  |
| --- | --- |
| parametr | charakterystyka [wymagania minimalne] |
| Wykrywanie i monitorowanie | Monitorowanie infrastruktury IT, w tym serwerów i usług.  System pozwala na monitorowanie zdefiniowanych zdarzeń, w tym zbieranie, analizowanie i wizualizację danych.  System jest przystosowany do przetwarzania danych typowych dla systemów teleinformatycznych:   * Adresy IP4 i IP6 * Nazwy DNS * Identyfikatory protokołów sieciowych np. SNMP, SSH, TELNET, IPMI, JPX, HTTP/HTTPS, VMWare * Porty * Nazwy i identyfikatory użytkowników * Nazwy i identyfikatory procesów * Nazwy i identyfikatory zasobów * Czasu * i innych   System umożliwia wykrywanie wszelkich problemów w infrastrukturze Zamawiającego i powiadamia wskazanych użytkowników |
| Interfejs i prezentacja danych | System zapewnia graficzny interfejs użytkownika dostępny wyłącznie za pomocą przeglądarki internetowej.  System wspiera generowanie mapy monitorowane środowiska uwzględniającej prezentację co najmniej urządzeń, portów, prędkości połączeń i nazw urządzeń.  System prezentuje dane na wykresach w czasie rzeczywistym.  System pozwala na tworzenie własnych wykresów gromadzących i prezentujących wiele danych.  Interfejs użytkownika wyodrębnia prezentację co najmniej następujących danych:   * problemy * hosty * mapy * usługi * SLA * Zasoby * Raporty * Kolekcje danych * Alerty * Administracja i zarządzanie, w tym zarządzanie użytkownikami.   System musi udostępniać ogólnodostępną wyszukiwarkę, która w łatwy sposób pozwala odnaleźć hosty, grupy i schematy.  System pozwala na tworzenie własnych motywów interfejsu użytkownika.  System pozwala na rebranding obejmujących co najmniej możliwość wstawienia własnego loga. |
| Zarządzanie monitorowanymi zasobami | System pozwala na zarządzanie użytkownikami korzystającymi z interfejsu przeglądarkowego.  Użytkownicy mogą pełnić różne role w systemie oraz należeć do wielu grup użytkowników.  Uprawnienia w systemie muszą pozwalać na przydzielenie dostępu do:   * dashboardu * monitoringu procesów, hostów, mapy * usług i weryfikacji poziomu SLA * zasobów w tym serwerów * raportów i notyfikacji * kolekcji gromadzonych danych * alertów * API   System umożliwia zarządzania hostami, w tym przydzielanie ich do grup i stosowanie dla nich wbudowanych standardowych schematów (templates) monitorowania.  System pozwala na definiowanie i zarządzanie monitorowanymi parametrami.  System oferuje minimum 50 monitorowanych parametrów obejmujących co najmniej następujące grupy/typy:   * Jądro systemu (kernel) * Monitorowanie logów * Parametry dotyczące sieci * Procesy * Czujniki sprzętowe * Parametry systemu * System plików * Pamięć * Strony internetowe   System pozwala na tworzenie własnych skryptów oraz definiowanych własnych triggerów wyzwalających zdarzenie za pomocą obsługiwanych przez system wyrażeń regularnych.  Wyrażenia muszą obsługiwać funkcje, ich parametry i operatory. Liczba oferowanych funkcji – min. 50 i operatorów – min. 10.  System musi posiadać możliwość tworzenia własnych schematów monitorowania.  System musi pozwalać na definiowanie pożądanych parametrów SLA.  System musi posiadać wbudowane narzędzia monitorowania środowiska VMWare |
| Raportowanie i alarmowanie | System pozwala na przesyłanie notyfikacji/powiadomień dla zdefiniowanych zdarzeń poprzez email z wykorzystaniem serwera/ usługi Zamawiającego |
| licencjonowanie | Zamawiający wymaga dostarczenia licencji wieczystej z prawem do aktualizacji. Licencja na System nie może narzucać jakichkolwiek dodatkowych wymagań dla Zamawiającego skutkujących ponoszeniem dodatkowych kosztów związanych z jej utrzymaniem.  Licencja musi obejmować wszystkie funkcjonalności zaoferowanego oprogramowania i pozwalać na monitorowanie dowolnej liczby urządzeń infrastruktury, serwerów i usług IT.  Licencja nie może w żaden sposób być przypisania do użytkownika, serwera czy maszyny. Nie może być także uzależniona od liczby rdzeni procesora.  Licencja musi pozwalać na zainstalowanie oprogramowania w dowolnej liczbie instancji – ma być licencją udzieloną na Zamawiającego, bez ograniczania liczby instalacji oprogramowania. |
| Wsparcie techniczne | Gwarancja producenta i wsparcie techniczne - nie później niż do 30.06.2026r. obejmująca:  dostarczanie aktualizacji Systemu, udzielanie konsultacji telefonicznych / mailowych w zakresie funkcjonowania i konfiguracji Systemu oraz jego rozszerzania |
| Minimalny zakres monitorowanych systemów i usług - źródła danych | W ramach wdrożenia Systemu monitorowaniem objęte zostaną następujące źródła zdarzeń:  Serwery i aplikacje kluczowych baz danych – 2 szt.  Serwer WWW – 2 szt. (www/bip)  Urządzenie brzegowe – 1 szt.  Usługa Activedirectory – 1 szt.  Serwer poczty elektronicznej 1 szt.  Switch (SNMP) – min. 10 szt.  Monitorowanie integracji z systemem ePUAP – 1 szt.  Monitorowanie integracji z systemem eDoręczeń – 1 szt.  Sumarycznie przewiduje się podłączenie nie więcej niż 15 źródeł danych rozumianych jako serwer/urządzenie sieciowe, generujących różne rodzaje zdarzeń w liczbie szacunkowo kilku tysięcy na dobę. |
| Zakres prac i wdrożenia | 1. Zebranie informacji dotyczących monitorowanej infrastruktury, monitorowanych źródeł danych. 2. Instalację i konfigurację systemu w zasobach informatycznych Zamawiającego – preferowane środowisko Linux 3. Uzgodnienie i wdrożenie sposobu backupu Systemu. 4. Dostarczenie licencji na System. 5. Uzgodnienie mechanizmów funkcjonalnych z Zamawiających oraz ich wdrożenie. 6. Przeprowadzenie instruktażu/warsztatu szkoleniowego w wymiarze 2h dla każdej grupy składającej się z nie więcej niż 5 pracowników. 7. Skonfigurowanie i uruchomienie mechanizmów powiadomień o zdarzeniach krytycznych. |

* 1. **Dostawa, wdrożenie, instalacja oprogramowania umożliwiającego bezpieczne przetwarzanie danych w środowisku hybrydowym: praca w Urzędzie, praca zdalna, współpraca z jednostkami podległymi, instruktaż z zakresu administracji i bieżącej obsługi dostarczonego systemu**

Przez wdrożenie systemu Zamawiający rozumie dostawę licencji, sprzętu/urządzeń, zaprojektowanie systemu oraz jego uruchomienie, a także przeprowadzenie instruktażu z jego obsługi.

System bezpiecznego przetwarzania danych w środowisku hybrydowym to rozwiązanie pozwalające na bezpieczne przetwarzanie danych zarówno lokalnie w ramach sieci wewnętrznej Zamawiającego, jak i pracy zdalnej pracowników oraz współpracy z innymi jednostkami. System musi zapewniać bezpieczną łączność między systemami zamawiającego oraz / lub jednostek oraz użytkownikami.

Zaproponowanie rozwiązanie powinno umożliwiać zamawiającemu standardami bezpieczeństwa, w szczególności w celu wypełnienia obowiązków wynikających z:

* Ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne,
* Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych,
* Ustawy z dnia 10 listopada 2020 r. o doręczeniach elektronicznych
* Rozporządzenia Ministra Cyfryzacji z dnia 5 października 2016 r. w sprawie zakresu i warunków korzystania z elektronicznej platformy usług administracji publicznej,
* Ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa,
* Ustawy z dnia 5 września 2016 r. o usługach zaufania i identyfikacji elektronicznej,
* Ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną,
* Ustawą z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach,
* Ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych.

|  |  |
| --- | --- |
| parametr | charakterystyka [wymagania minimalne] |
| Podstawowa wymagania | System musi zapewniać bezpieczną łączność między użytkownikami oraz systemami zgodnie z modelem zero trust networking z wykorzystaniem sieci typu „overlay” funkcjonującej w modelu mesh.  System musi zostać uruchomiony na infrastrukturze zamawiającego. |
| Architektura | System musi posiadać architekturę modułową, umożlwiającą rozdzielenie poszczególnych części Systemu i umieszczenie ich w różnych segmentach sieci zależnie od stopnia zaufania. Wymagany jest podział co najmniej na część sterującą zlokalizowaną wew. zaufanej sieci oraz na część brzegową – umieszoną w strefie zdemilitaryzowanej.  Część brzegowa musi umożliwiać powielanie w różnych segmentach sieci |
| Zarządzanie tożsamościami i autoryzacja: | System musi zapewniać Integracje z istniejącymi systemami Identity Provider (IdP) takimi jak LDAP, Active Directory, OAuth, i OpenID Connect.  System musi zapewniać możliwość tworzenia wielopoziomowych polityk dostępu opartych na tożsamości użytkownika, grupie, urządzeniu, aplikacji i lokalizacji.  System musi zapewniać zastosowanie silnego uwierzytelniania wieloskładnikowego (MFA). |
| Bezpieczeństwo połączenia | System musi zapewniać szyfrowanie end-to-end wykorzystujące bezpieczne algorytmy, takie jak AES-256, dla każdej transmisji danych oraz umożliwiać ustanowienie bezpiecznych tuneli dla poszczególnych aplikacji bez konieczności tworzenia VPN na poziomie całego urządzenia.  System musi posiadać wbudowaną obsługę infrastrukturę klucz publicznego (PKI) umożlwiającą zarządzenie i tworzenie bezpiecznych połączeń w modelu mTLS |
| Skalowalność i wydajność | Architektura systemu musi zapewniać łatwe dodawanie nowych użytkowników, aplikacji i usług bez wpływu na ogólną wydajność systemu.  System musi umożliwiać wykorzystanie edge computing do minimalizacji opóźnień i zwiększenia szybkości przetwarzania danych poprzez możliwość umieszczenia komponentów systemu blisko źródeł danych i użytkowników końcowych. |
| Interoperacyjność i wsparcie dla wielu chmur (Multi-cloud support) | System musi umożliwiać integracje z różnymi środowiskami chmurowymi, w tym AWS, Google Cloud, Azure oraz prywatnymi centrami danych oraz zapewniać spójną i bezpieczną komunikacje między różnorodnymi platformami i usługami, bez względu na ich lokalizację. |
| Monitoring i zarządzanie | System musi zapewniać zaawansowane narzędzia do monitorowania stanu sieci, wydajności połączeń oraz aktywności użytkowników.  System musi posiadać intuicyjny dashboard do zarządzania politykami, użytkownikami i zabezpieczeniami oraz umożliwiać zarządzanie konfiguracją z poziomu CLI. |
| Obsługa urządzeń końcowych | System musi umożliwiać instalacje klienta na urządzeniach końcowych użytkowników i wspierać n.w. platformy:  Microsoft Windows, MacOS, Linux, Android, IOS  Obsługa ww. platform musi być zapewniona w ramach realizacji niniejszego zamówienia, bez konieczności ponoszenia dodatkowych kosztów przez Zamawiającego.  System musi umożliwiać aktywacje urządzenia końcowego poprzez przekazanie tokenu JWT lub / oraz możliwość zeskanowania dedykowanego dla użytkownika QR kodu. |
| licencjonowanie | Zamawiający wymaga dostarczenia licencji wieczystej z prawem do aktualizacji. Licencja na System nie może narzucać jakichkolwiek dodatkowych wymagań dla Zamawiającego skutkujących ponoszeniem dodatkowych kosztów związanych z jej utrzymaniem.  Licencja musi obejmować wszystkie funkcjonalności zaoferowanego oprogramowania i pozwalać na monitorowanie dowolnej liczby urządzeń infrastruktury, serwerów i usług IT.  Licencja nie może w żaden sposób być przypisania do użytkownika, serwera czy maszyny. Nie może być także uzależniona od liczby rdzeni procesora.  Licencja musi pozwalać na zainstalowanie oprogramowania w dowolnej liczbie instancji – ma być licencją udzieloną na Zamawiającego, bez ograniczania liczby instalacji oprogramowania. |
| Wsparcie techniczne | Gwarancja producenta i wsparcie techniczne - nie później niż do 30.06.2026r. obejmująca:  dostarczanie aktualizacji Systemu, udzielanie konsultacji telefonicznych / mailowych w zakresie funkcjonowania i konfiguracji Systemu oraz jego rozszerzania |
| zakres realizacji zamówienia | W ramach wdrożenia Systemu zostanie zapewniona konfiguracja dla następującej liczby urządzeń / systemów:   1. Użytkownicy – maksimum 80 2. Systemy – maksimum 5 szt. |
| Zakres prac i wdrożenia | 1. Analiza infrastruktury informatycznej (sieci /systemów) zamawiającego oraz jednostek współpracujących w celu zaprojektowania optymalnej architektury systemu. 2. Instalację i konfigurację systemu w zasobach informatycznych Zamawiającego – preferowane środowisko Linux 3. Uzgodnienie i wdrożenie sposobu backupu Systemu. 4. Dostarczenie licencji na System. 5. Uzgodnienie mechanizmów funkcjonalnych z Zamawiających oraz ich wdrożenie. 6. Przeprowadzenie instruktażu/warsztatu szkoleniowego w wymiarze 2h dla każdej grupy składającej się z nie więcej niż 5 pracowników. 7. Skonfigurowanie i uruchomienie połączeń dla wskazanych użytkowników i systemów |

* 1. **Szkolenia specjalistyczne z zakresu cyberbezpieczeństwa dla administratorów IT wyznaczonych przez Zamawiającego – 2 osoby**

|  |  |
| --- | --- |
| parametr | charakterystyka [wymagania minimalne] |
| Szkolenie dla Administaratora z dostarczonego urządzenia UTM | Autoryzowane szkolenie producenta zaoferowanego urządzenia UTM.  Zakres podstawowy:   1. Rozpoczęcie pracy z urządzeniem  * Rejestracja w strefie klienta i dostęp zasobów * Rozpoczęcie pracy z urządzeniem i wprowadzenie do interfejsu administracyjnego * Ustawienia systemowe i uprawnienia administratorów * Instalacja licencji i aktualizacja systemu * Tworzenie kopii zapasowej i przywracanie konfiguracji  1. Zbieranie logów i monitorowanie  * Przedstawienie kategorii zbieranych logów * Wykresy historyczne i monitorowanie  1. Obiekty  * Typy obiektów oraz ich wykorzystanie * Obiekty sieciowe i obiekt typu „router”  1. Konfiguracja sieci  * Tryby pracy urządzenia * Typy interfejsów (Ethernet, modem, bridge, VLAN, GRETAP) * Typy routingu oraz ich priorytety  1. Translacja adresów sieciowych (NAT) 2. Translacja połączeń wychodzących (maskarada) 3. Translacja połączeń przychodzących (przekierowanie) 4. Translacja dwukierunkowa (jeden do jeden) 5. Filtrowanie ruchu sieciowego (Firewall) 6. Ogólne informacje dot. filtrowania ruchu i koncepcji śledzenia połączeń (Stateful inspection)  * Szczegółowy opis parametrów reguły Firewall * Kolejność przetwarzania reguł Firewall i NAT  1. Ochrona aplikacji  * Implementacja filtrowania URL dla ruchu http i https * Konfigurowanie skanowania antywirusowego i modułu Breach Fighter * Moduł IPS i stosowanie profili inspekcji  1. Użytkownicy i uwierzytelnianie 2. Konfiguracja usługi katalogowej  * Wprowadzenie do różnych metod uwierzytelniania (LDAP, Kerberos, Radius, certyfikat SSL, SPNEGO, SSO) * Rejestracja użytkowników * Uwierzytelnianie użytkowników za pomocą portalu uwierzytelniania  1. Wirtualne sieci prywatne (VPN)  * Koncepcje i ogólne informacje dotyczące protokołu IPSec VPN (IKEv1 i IKEv2) * Tunele Site-to-Site z wykorzystaniem klucza współdzielonego (PSK) * Tunele VTI  1. SSL VPN  * Zasada działania * Konfiguracja  1. Szkolenie online min. 24h   Zakres rozszerzony:   1. Szczegółowe omówienie działania modułu IPS od Stormshield  * Różnice pomiędzy IPS a IDS * moduł IPS * Różne tryby analizy * Profile oparte na protokołach i aplikacjach  1. Infrastruktura klucza publicznego  * Podstawy szyfrowania symetryczneg - i asymetrycznego * Typy szyfrowania * Infrastruktura klucza publiczneg - w rozwiązaniach Stormshield * Tworzenie urzędu certyfikacji, certyfikatów serwera i użytkowników  1. SSL Proxy  * Zasada działania * Konfiguracja SSL Proxy * Zaawansowana konfiguracja tuneli IPSec VPN * Szczegółowy opis działania mechanizmu NAT traversal * Obsługa funkcji DPD (Dead Peer Detection) * Architektura sieci VPN typu „gwiazda” i „mesh” * NAT w sieciach IPSec VPN * Konfiguracja zapasoweg - tunelu IPSec VPN * Konfiguracja tuneli Site-to-Site w oparciu - certyfikaty * Konfiguracja tuneli dla użytkowników mobilnych (Client-2-Site)  1. GRE i GRETAP  * Zasada działania * Konfiguracja i instalacja  1. Transparentne uwierzytelnianie użytkowników  * Zasada działania * Metoda uwierzytelniania SPNEGO * Metoda uwierzytelniania oparta na certyfikatach SSL  1. Wysoka dostępność (HA)  * Zasada działania * Kreator umożliwiający tworzenie i konfigurowanie klastra HA * Konfiguracja interfejsu sieciowego * Zaawansowana konfiguracja   Szkolenie online min. 24h  Możliwość otrzymania certyfikatu po zdaniu egzaminu |
| Szkolenie  zarządzanie IT | Zakres szkolenia:   * Monitorowanie krytycznych dla organizacji urządzeń, usług czy procesów tak aby posiadać odpowiednią wiedzę o architekturze sieci firmowej, działaniu poszczególnych jej komponentów oraz jej wydajności i pojemności. * monitorowanie niejednolitej konfiguracji programowej i sprzętowej stacji, audyt oprogramowania czy plików multimedialnych, podnoszący umiejętności w obszarze zarządzania środkami trwałymi. * Monitorowania aktywność użytkowników, tak aby można było szybko i jednoznacznie analizować ich pracę a jednocześnie brać o bezpieczeństwo organizacji. * Ustandaryzowanie i rozliczalność komunikacji „użytkownik-IT”, baza wiedzy dla pracowników, automatyzacja procesów związanych z obsługę zgłoszeń serwisowych. * Zarządzania nośnikami zewnętrznymi, rozliczania pracy z nimi oraz rozliczanie pracy na plikach wspólnych. * Szkolenie zakończone certyfikatem dla Administrator. * czas szkolenia: dwa dni robocze w siedzibie dostawcy szkolenia |
| Szkolenie: wirtualizacja | Zakres szkolenia:   1. Przegląd Wirtualizacji  * Podstawy wirtualizacji * Wirtualizacja i jej komponenty * Zastosowania i korzyści * Architektura i terminologia.  1. Instalacja i konfiguracja wirtualizatora  * Wprowadzenie do wirtualizatora. * Wymagania i instalacja. * Konfiguracja hosta.  1. Wdrażanie i konfiguracja wirtualizacji  * Zarządzanie scentralizowane. * Architektura i usługi. * Licencjonowanie. * Zarządzanie inwentarzem. * Role i uprawnienia.  1. Konfiguracja sieci  * Podstawy sieci wirtualnych. * Standardowe i rozproszone przełączniki.  1. Konfiguracja przechowywania danych  * Podstawy przechowywania danych. * VMFS i NFS Datastores. * Fibre Channel i iSCSI Storage.  1. Wdrażanie maszyn wirtualnych  * Tworzenie i zarządzanie VM. * Szablony i biblioteki zawartości.  1. Zarządzanie Maszynami Wirtualnymi  * Migracja Maszyn Wirtualnych. * Zarządzanie Snapshots.  1. Wdrażanie i Konfiguracja Klastrów  * Przegląd Klastrów. * Architektura HA * Konfiguracja HA.   Szkolenie online min. 14h |
| Szkolenie z dostarczonego systemu operacyjnego w serwerach | Zakres szkolenia:   1. Instalowanie i konfigurowanie kontrolerów domeny 2. Zarządzanie obiektami w usługach AD DS 3. Zarządzanie zaawansowaną infrastrukturą AD DS 4. Implementowanie lokacji usług AD DS oraz konfigurowanie replikacji i zarządzanie nią 5. Wdrażanie zasad grupy 6. Zarządzanie ustawieniami użytkownika za pomocą zasad grupy 7. Zabezpieczanie usług domenowych Active Directory 8. Wdrażanie usług AD CS i zarządzanie nimi 9. Wdrażanie certyfikatów i zarządzanie nimi 10. Wdrażanie i administrowanie usługami AD FS 11. Wdrażanie i administrowanie usługi AD RMS 12. Monitorowanie usług AD DS, zarządzanie nimi oraz odzyskiwanie danych   Szkolenie online min. 40h  Certyfikat ukończenia szkolenia |

* 1. **Szkolenia z zakresu cyberbezpieczeństwa dla pracowników Zamawiającego – 80 osób**

|  |  |
| --- | --- |
| parametr | charakterystyka [wymagania minimalne] |
| szkolenie cyberbezpieczeństwo | Wykonawca przeprowadzi szkolenia dla Pracowników Urzędu w grupach nie większych niż 20 osób. Wielkość grup będzie uzależniona od liczby osób, które w tym samym czasie będą mogły opuścić stanowisko pracy bez zakłócania ciągłości działania Urzędu.  Szkolenia muszą być przeprowadzone niezależnie dla grup:   1. Pracowników nie będących informatykami - czas trwania szkolenia co najmniej 6 godzin zegarowych. 2. Kadry Kierowniczej – czas trwania szkolenia co najmniej 12 godzin zegarowych. 3. Specjalistów IT / Administratorów – czas trwania szkolenia co najmniej 12 godzin zegarowych.   Szkolenia odbędą się w formie wykładów połączonych z ćwiczeniami praktycznymi.  Minimalny zakres szkolenia:   1. wszyscy pracownicy 2. podstawowe wiadomości w zakresie bezpieczeństwa informacji, z uwzględnieniem regulacji wewnętrznych oraz wymagań rozporządzenia KRI;  * wewnętrzne procedury w obszarze bezpieczeństwa informacji cyberbezpieczeństwa * wymagania dla pracowników wynikające z KRI, uoKSC oraz RODO * System Zarządzania Bezpieczeństwem Informacji w praktyce  1. przegląd zagrożeń i zasady bezpiecznego korzystania z Internetu;  * ochrona informacji i prywatność w Internecie * ransomware jako poważne zagrożenie dla JST * phishing, oszustwa i wyłudzenia z uwzględnieniem oszustwa typu BEC (Business E-mail Compromise) * cyberhigiena, w tym bezpieczeństwo urządzeń i bezpieczeństwo fizyczne * bezpieczne hasła i uwierzytelnienie dwuskładnikowe * wewnętrzne zalecenia i rekomendacje, w tym sposoby reakcji na incydenty bezpieczeństwa  1. kadra kierownicza 2. podstawy prawne cyberbezpieczeństwa 3. wymogi wynikające z KRI, uoKSC i RODO 4. przegląd znanych typów ataków na JST 5. przegląd nowoczesnych narzędzi i usług cyberbezpieczeństwa (jako wsparcie procesu zakupowego) 6. zarządzanie ryzykiem w bezpieczeństwie informacji i obszarach technicznych. 7. jak skutecznie wdrożyć SZBI 8. ciągłość działania – dlaczego jest istotna i jak ją wdrożyć 9. współpraca w ramach s46 10. identyfikowanie zagrożeń – jak wdrożyć odpowiednie zabezpieczenia 11. specjaliści IT 12. podstawy bezpieczeństwa sieci 13. aspekty techniczne najpopularniejszych ataków i metody reagowania 14. zabezpieczanie poczty elektronicznej 15. zabezpieczanie serwisów www 16. ochrona przed atakami DDoS 17. profilaktyka cyberzagrożeń ze szczególnym uwzględnieniem zarządzania kopiami zapasowymi 18. przegląd źródeł wiedzy o zagrożeniach 19. podstawy zabezpieczenia ciągłości działania 20. identyfikacja podatności i aktualizacja oprogramowania 21. zarządzanie incydentem |
|  | 1. Szkolenia prowadzone będą w języku polskim na podstawie zaakceptowanego przez Zamawiającego dziennego harmonogramu prac z dołączonym zakresem merytorycznym, stacjonarnie, w siedzibie Urzędu. 2. Zamawiający wymaga prowadzenia dokumentacji Listy obecności uczestników szkolenia 3. Uczestnicy otrzymają Certyfikat ukończenia szkolenia |